REMARKS

This paper is responsive to the Final Office Action of November 19, 2009. Reconsideration and allowance of **claims 1-4 and 8-16** are requested.

The Office Action

Claims 1 and 8 were rejected under 35 U.S.C. 103(a) as being unpatentable over Jutizi et al. (U.S. Patent Application Publication No. 2003/0005301) in view of Parr (U.S. Patent No. 5,287,374).

Claims 2-4 and 9-11 were rejected under 35 U.S.C. 103(a) as being unpatentable over Jutzi in view of Parr in further view of Suzuki (U.S. Patent No. 6,463,445).

Claims 12-13 were rejected under 35 U.S.C 103(a) as being unpatentble over Jutzi in view of Parr in further view of Suzuki and in further view of Matyas, Jr. (U.S. Patent No. 7,010,689).

Claim 14 was rejected under 35 U.S.C. 103(a) as being unpatentable over Jutzi in view of Parr in further view of Suzuki and in further view of Ko et al. (U.S. Patent Application Publication No. 2003/0100299).

Claim 15 was rejected under 35 U.S.C. 103(a) as being unaptentable overt Jutzi in view of Parr in further view of Suzuki in further view of Henderson et al. (U.S. Patent No. 6,353,666) and in further view of Weinstein et al. (U.S. Patent No. 7,233,688).

Claim 16 was rejected under 35 U.S.C. 103(a) as being unpatentable over Jutzi in view of Parr in further view of Suzuki in further view of Haitsma et al. (Robust Audio Hashing Content Identification).

Finality of Office Action is Premature

The finality of the Office Action is premature because the Examiner made a new ground of rejection against **claims 1 and 8** in the November 19, 2009 Office Action that was not necessitated by Applicant's Amendment C. Specifically, in Amendment C, **claims 1 and 8** were not substantively amended. No additional subject matter was added and none was deleted. Because the substance of **claims 1 and 8** was not amended, it is submitted that the new ground of rejection which Examiner applied

against **claims 1 and 8** in the November 19, 2009 Office Action was not necessitated by Applicant's Amendment C and therefore the Finality of the November 19, 2009 Office Action was premature.

The Claims Distinguish Patentably Over the References of Record

Claims 1 and 8 are patentable over Jutzi in view of Parr.

More specifically, regarding **claim 1**, Jutzi et al. does not disclose deriving a fingerprint from the decoded signal, comparing said fingerprint with fingerprints stored in a database, and concluding that the encoded signal has been encoded with said particular type of encoder if the derived fingerprint corresponds to one of the fingerprints stored in the database. The Office Action refers Applicant to paragraphs [0047], [0055], and [0056] of Jutzi which discloses an apparatus and method for performing security authentication of a content driver in order to determine whether a content driver is secure. More specifically, a playback user interface enables a user to request playback of a received encrypted content stream. Once received, the encrypted content stream is provided to a content reader interface that provides the encrypted content stream to a content driver. The content reader interface directs the content driver to stream the encrypted content to a content decryption component in order to decrypt the received encrypted content. In order for the content driver to receive the decrypted content from the content decryption component, the content driver must achieve successful security authentication from the content decryption component.

In determining whether a content driver is secured, the content decryption component decrypts the encrypted content stream received from the content driver. Next, the content decryption component calculates a hash value of code segments that perform functionality of the content driver. Once calculated, the content decryption component selects a stored run-time digital signature of a run-time image of the content driver that represents the program instructions to perform the functionality of the content driver. Next, the content decryption component decrypts the selected digital signature to reveal a run-time hash value of a run-time image of the content driver. Finally, it is determined whether the calculated hash value matches the run-time hash value to determine if the content driver is secure. The Office Action asserts in the Response to Arguments that Jutzi clearly discloses "a fingerprint has been

derived from an encoded signal has a particular type of encoder if the compared fingerprint matches another in the database." Jutzi et al. discloses authenticating content drivers by comparing the calculated hash value of a content driver with a run time hash value to determine whether a content driver is secure. Neither the content driver nor content decryption component of Jutzi determines the type of encoder that was used to encode the received encoded content stream or the digital signature of the run time image. It is respectfully submitted that Jutzi et al. does not disclose deriving a fingerprint from a decoded signal and using the fingerprint to determine if the decoded signal was encoded with a particular type of encoder if the fingerprint corresponds to a fingerprint stored in a database.

The Office Action additionally asserts that Parr also discloses deriving a fingerprint from a decoded signal and using the fingerprint to derive if the decoded signal was encoded with a particular type of encoder if the fingerprint corresponds to a fingerprint stored in a database in Col. 1 lines 25-29, Col. 2 lines 30-40, and Col. 3 lines 49-54. These portions of Parr disclose identification of an encoder type through the observation of the encoded data received. More specifically, Parr discloses transmitting data encoded by introducing redundancy into the encoded signal sequence by convolutional forward error correction (FEC) coding. The received encoded signal, with errors, is applied to an encoder identifying circuit. The encoder identifying circuit observes the encoded sequence of the received encoded signal to determine the particular type of encoder used. Parr discloses determining the type of encoder *without decoding* the received signal. Parr does not disclose decoding the received signals and determining the type of encoder from a fingerprint that is derived from the decoded signal. There is no evidence or suggestions in Jutzi et al., Parr, or the combination of deriving a fingerprint from a decoded signal and comparing the fingerprint to other fingerprints stored in a database to determine a type of encoder that encoded the signal, as advanced by the Examiner, except from using Applicant's claims as a template through a hindsight reconstruction of the Applicant's claims.

Accordingly it is submitted that independent **claim 1** and **claims 2-4** that depend therefrom distinguish patentable over the references of record.

Claim 8 calls for deriving a fingerprint from a decoded signal and then comparing the fingerprint with other fingerprints stored in the server's database to determine whether the signal was encoded with a particular type of encoder. It is respectfully submitted that Jutzi et al., Parr, or the combination does not teach or

disclose deriving a fingerprint from a decoded signal and comparing the selected fingerprint with fingerprints in a server's database to determine a type of encoder used to encode the signal.

Accordingly it is submitted that independent **claim 1** and **claims 2-4** that depend therefrom distinguish patentable over the references of record.

Claims 2-4 and 9-11 are patentable over Jutzi in view of Parr in further view of Suzuki.

More specifically **claim 3** calls for awarding the client if the server concluded that the received and decoded signal had been encoded with said particular type of encoder. The Office Action assets Suzuki discloses this limitation in Col. 11 lines 3-5 and Col. 6 lines 52-67 which discloses a system and method for encoding and decoding multimedia information including identifying the encoding formatted used in the multimedia bitstream originated by a content server. More specifically, Suzuki discloses a content server sending the identification of the encoded format used to encode a particular bitstream to a client without requiring the data stored on the content server be compatible with the decoding technique supported by the client. Neither Jutzi et al., Parr, Suzuki, nor the combination teach or disclose awarding the client if the server determines that the signals had been encoded with the particular type of encoder.

Claims 4 calls for the step of awarding to comprise retrieving from the database metadata associated with the signal, and transmitting said metadata to the client. Neither Jutzi et al., Parr, Suzuki, nor the combination teach or disclose giving the client the database metadata associated with the signal if the server concluded that the signal has been encoded with the particular type of encoder.

Claim 9 calls for calls for a fingerprint extraction unit configured to extract the fingerprint from a decoded file and a processor configured to compare the extracted fingerprint with other fingerprints stored in a database. It is respectfully submitted that Jutzi et al., Parr, Suzuki, or the combination does not teach or disclose comparing fingerprints extracted from a decoded file with fingerprints stored in the server's database to determine the type of encoder used to encode the signal.

Claim 10 calls for the processor to communicate an award to the client in response to the server concluding that the received encoded files have been encoded using the selected encoding operation. Neither Jutzi et al., Parr, Suzuki, nor the

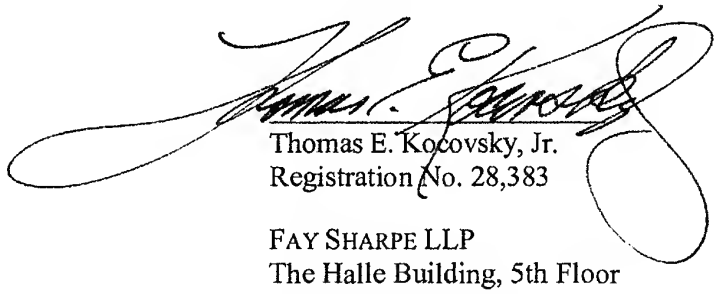
Claim 11 calls for the processor to communicate an award to the client in response to the server concluding that the received encoded files have been encoded with an encoder that corresponds to the decoder of the server. The award includes metadata associated with the encoded file, the metadata being transmitted to the client. Neither Jutzi et al., Parr, Suzuki, nor the combination teach or disclose giving the client the database metadata associated with the signal if the server concluded that the signal has been encoded with the particular type of encoder.

CONCLUSION

For the reasons set forth above, it is submitted that **claims 1-4 and 8-16** (all claims) distinguish patentably over the references of record and meet all statutory requirements. An early allowance of all claims is requested.

In the event the Examiner considers personal contact advantageous to the disposition of this case, the Examiner is requested to telephone Thomas Kocovsky at 216.363.9000.

Respectfully submitted,



Thomas E. Kocovsky, Jr.
Registration No. 28,383

FAY SHARPE LLP
The Halle Building, 5th Floor
1228 Euclid Avenue
Cleveland, OH 44115-1843
Telephone: 216.363.9000 (main)
Telephone: 216.363.9122 (direct)
Facsimile: 216.363.9001
E-Mail: **tkocovsky@faysharpe.com**